verslags overleg DJI-JIO Citrix/Netscalers

Omschrijving	overleg DJI-JIO Citrix/Netscalers
Vergaderdatum en -tijd	22 juli 2025, 11.00 uur
Vergaderplaats	Gouda/WebEx
Aanwezig	5.1.2e 5.1.2e , 5.1.2e 5. 5.1.2e , 5.1.2e 5.1.2e , 5.1.2e 5.1.2e , 5.1.2e 5.1.2e ; 5.1.2e 5.1.2e , 5.1.2e 5.1.2e (notulist)

Justitiële ICT Organisatie
Strategie en Bedrijfsvoering,
Bestuur en Strategie
IB&P

Contactpersoon
5.1.2e 5.1.2e
5.1.2e

T 088 07 57100

Datum
22 juli 2025

Notulist
5.1.2e

Agenda:
1. Hoofdlijnen en context situatie
2. Beantwoorden aanvullende vragen
3. Handelingsperspectief

Hoofdlijnen en context situatie

5.1.2e 5.1.2e (SOC JIO) geeft een overzicht van de gebeurtenissen tot nu toe en de stand van zaken. Op 18 en 26 juni zijn alerts door het NCSC binnengekomen dat de Citrix Netscalers een kwetsbaarheid bevat die actief wordt misbruikt en het advies is om direct te patchen. Beide keren is dit gedaan. Op 8 juli komt er een script van Citrix beschikbaar die controleert of er nog iets op de Netscaler staat wat daar niet thuishoort. Er wordt een binary en een webshell gevonden en die worden verwijderd. Daarna wordt er geen verkeer meer waargenomen via die route. N.a.v. berichten over het OM en op basis van IOC's die door het NCSC worden gedeeld op 17 juli wordt door het SOC JIO contact opgenomen met het NCSC en SOC JenV. Hierna wordt in het weekend (19 juli) contact opgenomen met een externe partij die forensisch onderzoek gaat doen. Samen met Solvinity (de beheerpartij van de Netscalers), de externe forensische partij, SOC JenV en het NCSC en medewerkers van JIO wordt gewerkt aan het identificeren van het probleem. Dat is tot heden (22 juli) het geval, het onderzoek is nog steeds bezig en de verwachting is dat dit nog wel dagen kan duren. Dinsdag 22 juli zijn ook de politie (HTC, High Tech Crime) en het NCSC aangehaakt om met hun expertise te ondersteunen.

Wat is er gevonden:
1. Een verdachte binary
2. Een php webshell
3. Er is verkeer gezien van de besmette Netscaler naar twee andere netscalers.

Er zijn 5.1.2h Netscalers. Alle netscalers zijn gecontroleerd. Daarvan is er 1 gevonden die besmet is (met het verdachte bestand en de webshell). Dit is een Netscaler 5.1.2h Er zijn ondertussen veel loggings bekeken maar er is nog geen verder spoor gevonden. Begin mei is de Netscaler een paar keer gecrasht en daar zijn crash-dumps van die met Citrix zijn gedeeld. Citrix heeft geadviseerd om de Netscaler te upgraden en dat is gedaan. In de crash-dump van 8 mei is er nog geen webshell te zien. In de crashdump van 26 mei is de webshell wel aanwezig. Dit betekent dat de webshell er al was voordat de patch werd gereleased. Er wordt nu gekeken of de exacte datum kan worden gevonden om vandaar het spoor beter te kunnen traceren.

Het onderzoek loopt langs een 3 sporen aanvalsplan:
1. Verder onderzoek op gecompromitteerd systeem en vergelijkbare systemen die mogelijk ook kwetsbaar waren
2. Onderzoek van direct omliggende systemen die een aanvaller had kunnen aanvallen
3. Onderzoek op de digitale werkplek-omgeving die de aanvaller mogelijk had kunnen overnemen

Dit loopt nu voornamelijk langs logdata 5.1.2h, backups, crashdumps en geheugendumps.

Aanvullende vragen:
Q: Is er contact geweest met de Unit Weerbaarheid van de AIVD?
A: Nee nog niet. Vanuit de BVC-rol is wel contact met de BVA van JenV, via die lijn kan de AIVD worden benaderd.
5.1.2e geeft aan dat hij een naam van een contactpersoon van de AIVD kan geven.

Q: Hoe lang gaat het onderzoek duren?
A: Dat is nu nog niet te zeggen.

Q: Wordt er rekening gehouden met het forensisch beeld? Bijvoorbeeld verlies van data bij verwijderen van sporen?
A: Ja en Nee. 5.1.2f probeert zo veel mogelijk veilig te stellen maar er wordt ook nog gewerkt op de omgeving. Er wordt geen forensische kopie gemaakt, dat is niet mogelijk.

Q: Is er aangifte gedaan?
A: Nog niet, dat wordt vanmiddag gedaan. (*Post-meeting note: dit is ook gebeurd*)

Q: is er contact met het OM geweest over deze casus?
A: Ja, er is gesproken met de teamlead SOC van het OM. De situatie daar is vergelijkbaar met die van JIO. Er is daar tot nu toe nog niets gevonden.

Q: Welke functionele systemen zijn geraakt?
A: Dat is nu nog niet te zeggen, dat moet uitgezocht worden.

Q: Welke omgevingen/domeinen zijn geraakt?
A: De besmette Netscaler heeft connecties met 5.1.2h en de Netscalers waarmee van de besmette Netscaler contact is gezocht met de twee andere Netscalers hadden contact met 5.1.2h 5.1.2h

Q: Welke opdrachtgevers zijn geraakt?
A: Er is 1 Netscaler gecompromitteerd, maar we zijn nu via de pentesters van JIO aan het uitzoeken waar je op uit kunt komen

Handelingsperspectief
- Wat doen we als we iets aantreffen
- Hoe garanderen we de dienstverlening

Opties:
1. Dichtzetten proxy servers (o.b.v. whitelisting/blacklisting), hierbij kan de dienstverlening zo goed mogelijk doorgaan
2. Monitoring aanscherpen
    a. Upgrade Domain Controllers versneld oppakken. (staat nu nog ingepland in september) zodat 5.1.2h erop geïmplementeerd

worden. (voor logging) en/of tussentijds agents op de huidige versie van de Domein Controllers plaatsen.

b. Eind volgende week worden de nieuwe 5.1.2h configurations op de DWO geïnstalleerd.

c. Logging van de netscalers op het SIEM aansluiten, dat is in gang gezet. Verwachting is dat het deze week is geregeld.

3. Wachtwoorden resetten van nieuwe accounts vanaf 8 mei.

Aanvullende vragen

Q Worden ook buitenlandse IP's geblacklist?
A: Nog niet, nemen we mee

Q: Hoe makkelijk is het om de wachtwoorden te vervangen?
A: Precies is niet te zeggen, het zal ook een enorme druk bij de service desk geven. We gaan het uitzoeken

Q: Zijn er al analyses gedaan op de verschillende scenario's?
A: Nog niet.

Q: Wie bepaalt hoe de Domein Controllers worden geüpgraded?
A: JIO, dat zit al in de lopende LCM

Q: Wanneer wordt het besluit genomen om van het netwerk af te gaan
A: Een besluit wordt genomen op bestaande informatie en in samenspraak met de opdrachtgevers. Op basis van de huidige informatie lijkt het nog niet aan de orde

Q: Kan er dagelijks een stand van zaken worden gegeven/verstuurd
A: Ja, dat gaan we iedere ochtend rond 09:00 proberen rond te sturen.